Scantegrity II Municipal Election at Takoma Park: The First E2E Binding Governmental Election with Ballot Privacy

Richard Carback
UMBC CDL
Baltimore, MD 21250
carback1@umbc.edu

David Chaum

Jeremy Clark
University of Waterloo
Waterloo, Ontario N2L 6R5
j5clark@cs.uwaterloo.ca

John Conway
UMBC CDL
Baltimore, MD 21250
conwayj1@umbc.edu

Aleksander Essex
University of Ottawa
Ottawa, Ontario K1N 6N5
aesse083@site.uottawa.ca

Paul S. Herrnson
CAPC, UMCP
College Park, MD 20742
pherrnson@capc.umd.edu

Travis Mayberry
UMBC CDL
Baltimore, MD 21250
tm3@umbc.edu

Stefan Popoveniuc
GW
Washington, DC 20052
poste@gwu.edu

Ronald L. Rivest
MIT CSAIL
Cambridge, MA 02139
rivest@mit.edu

Emily Shen
MIT CSAIL
Cambridge, MA 02139
eshen@csail.mit.edu

Alan T. Sherman
UMBC CDL
Baltimore, MD 21250
sherman@umbc.edu

Poorvi L. Vora
GW
Washington, DC 20052
poorvi@gwu.edu

Abstract

On November 3, 2009, voters in Takoma Park, Maryland, cast ballots for mayor and city council members using the ScantegrityII voting system—the first time any *end-to-end (e2e)* voting system with ballot privacy has been used in any binding governmental election. This case-study describes how we carried out this complex engineering feat involving improved design and implementation of a novel cryptographic voting system, streamlined procedures, agreements with the City, and assessments of the experiences of voters and poll workers.

The election with 1722 voters from six wards involved paper ballots with invisible-ink confirmation codes, instant-runoff voting with write-ins, early and absentee (mail-in) voting, dual-language ballots, provisional ballots, privacy sleeves, any which-way scanning with parallel conventional desk-top scanners, end-to-end verifiability based on optional web-based voter verification of votes cast, a full hand recount, thresholded authorities, three independent outside auditors, full transparency, fully disclosed software, and exit surveys for voters and pollworkers.

Despite some glitches, the use of Scantegrity II was a success, demonstrating that e2e cryptographic voting systems can be effectively used and well accepted by the general public.

1 Introduction

The November 2009 municipal election of the city of Takoma Park, Maryland, was a milestone in election history. It was the first time that anyone was able to verify that the votes were counted correctly in a secret ballot election for public office without having to be present for the entire proceedings. This is a significant improvement over the transparency of perhaps any other governmental election providing ballot secrecy. This article is a case study of the Takoma Park election, describing what was done—from the time the Scantegrity Voting System Team (SVST) was approached by the Takoma Park Board of Elections in February 2008, to the last cryptographic election audit in December 2009—and what was learned. While the paper provides examples of survey results, the focus of this paper is not usability only but the broad engineering process of taking a new cryptographic paradigm and bringing it to solve—for the very first time—a complex practical problem involving technology, procedures, and laws so as to considerably improve election integrity while protecting ballot secrecy.

With the Scantegrity voting system, each voter could check that her individual votes were recorded correctly (without revealing how she voted, an essential property of elections) simply by consulting the city's website. Voters mark paper ballots with pens, filling the oval for the candidates of their choice. These ballots are handled as traditional ballots, permitting all the usual automated and manual counting, accounting, and recounting[1]. Additionally, the *Scantegrity II* voting system provides a layer of integrity-protection through its unique innovation of invisible-ink confirmation codes. When voters mark ballot ovals using a special decoding pen, confirmation codes printed in invisible ink are revealed. Interested voters can note down these codes to check them later on the election website. An important property of the codes is that they are generated randomly for each race and each ballot, and hence do not reveal the corresponding vote. Further, false claims of missing or manipulated codes are recognizable. The final tally is computed from the codes, and the system provides a public digital audit trail of the computation on the election website.

The public audit trail implies that election audits are not restricted to privileged individuals and can be performed by voters and other interested parties. This fact enables the strong integrity properties of the system. Those who developed or operated the system are unable to significantly falsify the outcome without an overwhelming probability of audits failing [10]. The other side of the issue of integrity, also solved by the system, is that false claims of impropriety in the recording and tally of the votes are readily revealed to be false[2].

Perhaps most important is the property that the election officials and voters surveyed seemed to appreciate the system. Since voters who do not wish to verify can simply proceed as usual, ignoring the codes revealed in the filled ovals, the system is least intrusive for these voters. Those voters who did check their codes, and even many who did not, seem to appreciate the opportunity. Similarly, the amount of extra work needed by officials to post the various values during preparation for and after the election is acceptable compared to the promise of improved voter satisfaction and indisputability of the outcome. Indeed, discussions are ongoing with the Board of Elections of the city regarding continued use of the system in future elections.

It should also be pointed out that all the software used in the election, from ballot authoring, printing, scanning and tally, was published well in advance of the election as commented, buildable source code, which may be a first in its own right. Moreover, commercial off-the-shelf scanners were adapted to receive ballots in privacy sleeves from voters, making the overall system inexpensive and perhaps preferable compared to those based on dedicated scanners without such sleeves.

[1] The system does not rely on automation at the polling place (since it can fall-back to "central scan", where ballots are transported to a central scanning location). For the Takoma Park election, scanners used by voters at the polling place provided immediate availability of preliminary results.

[2] Note that a threat not addressed and present in all paper ballot systems without automation is that additional marks could be added to ballots by those with special access, although such attacks are made more difficult by Scantegrity.

Organization of this case study This paper describes the entire process of adapting the Scantegrity II system to handle the Takoma Park election, including the running of the mock election, printing the special ballots with invisible-ink confirmation codes, actually running the election, and verifying that the election outcome was correct.

Section 2 describes in more detail the setting for the election: giving details about Takoma Park and their election requirements. Section 3 gives more details of the Scantegrity II voting system, including a description of how one can "audit" an election run with Scantegrity II.

Section 4 provides an overview of the implementation of the Scantegrity II voting system for the November 3, 2009 Takoma Park municipal election, including the scanner software, the cryptographic back-end, and the random-number generation routines.

Section 5 describes the mock election that was run in April, 2009, and some of the improvements that were made to the Scantegrity II design as a consequence (better privacy sleeve, better scanner architecture, better voter flow at pollsite), in preparation for the actual election in November.

Section 6 details the steps taken to prepare for the actual election, including the design and printing of the ballots, preparing instructional materials for voters and pollworkers, and arranging for independent parties to audit all stages of the election itself. Section 7 gives a chronological presentation and timeline of the steps taken to run the November election, including the outcome of the voter verification and the audits. Section 8 gives the results of the election, with some performance and integrity metrics.

Section 9 reports some results of the exit surveys taken of voters and pollworkers.

Section 10 discusses the high-level lessons learned from this election, Section 11 overviews related work, and Section 12 provides some conclusions.

2 The Setting

Voting systems are among the most difficult kinds of information systems to implement. Most voting system users, *i.e.,* the voters, are not trained, and elections happen infrequently. Voter privacy requirements preclude the usual sorts of feedback and auditing methods common in other applications, such as banking. Also, government regulations and pre-existing norms in the conduct of elections are difficult to change.

These issues can pose significant challenges when deploying new voting systems, and it is therefore useful to understand the setting in which our experiment took place.

About Takoma Park. The city of Takoma Park is located in Montogomery County, Maryland, across the city line with Washington, D.C, and is governed by a City Council consisting of a mayor and a six-member City Council. The city has about 17,000 residents[3] and almost 11,000 registered voters [28, pg. 10]. A seven-member Board of Elections conducts local elections in collaboration with the City Clerk. The city had used hand counts and optical scan voting in previous municipal elections, as well as DREs for state elections.

Instant Runoff Voting (IRV) Takoma Park has used IRV in municipal city elections since 2006. IRV is a ranked choice system where each voter assigns each candidate an ordering according to her preferences. The rules[4]. used by Takoma Park (and the Scantegrity software) for counting IRV ballots are relatively standard; we omit further discussion for lack of space.

[3] See `http://www.takomaparkmd.gov/about.html`.

[4] For the exact laws used by Takoma Park, see page 22 of `http://www.takomaparkmd.gov/code/pdf/charter.pdf` . Section (f), concerning eliminating multiple candidates, was used in our implementation for tie-breaking only.

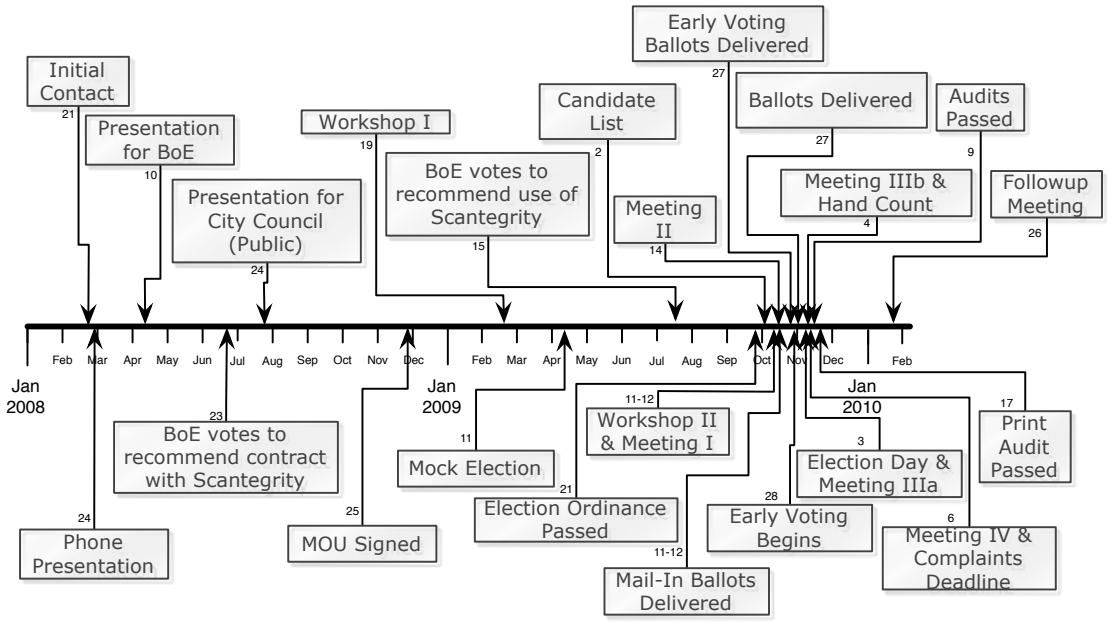


Figure 1: Takoma Park 2009: Timeline Illustration. Each box represents an event, and the numbers next to each box are the day(s) the event took place during the indicated month.

Agreement with the City In order to use Scantegrity in the election, Takoma Park required a signed agreement which we called a Memorandum of Understanding (MOU). In the MOU, the we agreed to provide equipment, software, training assistance, and technical support. The City of Takoma Park (City) would provide election-related information on the municipality, election workers, consumable materials, and perform or provide all other election duties or materials not provided by us. No goods or funds were exchanged.

The MOU included a mock election in April 2009, in which we demonstrated the ability to carry out the official election in November. Following this test, the City Clerk and the Takoma Park Board of Elections (BoE) had the option to determine if it continued to have confidence in our ability to provide software and support for the election, including performing any modifications revealed to be necessary by the mock election, and, if so, then the City Clerk and BoE would recommend that the City Council adopt an ordinance designating the Scantegrity II election system as the voting system to be used in the November 2009 Takoma Park municipal election.

If approved by the city council, the election was to be conducted in compliance with all applicable laws and policies. This included using Instant Runoff Voting as defined by the City of Takoma Park Municipal Charter. We also agreed to pursue and accessible ballot-marking device for the election.

Timeline Scantegrity was approached by the Takoma Park Board of Elections in late February 2008, and, after considering other voting systems, the Board voted to recommend a contract with Scantegrity in June 2008 (see Figure 1). Following a public presentation to the City Council in late July 2008, the MOU was signed in late November 2008, about nine months after the initial contact.

The SVST held an open workshop in February 2009 to discuss the use of Scantegrity in both the mock and real elections. This workshop was held at the Takoma Park Community Center and was attended by Board of Election members, the City Clerk, current members (and a retired member) of the Montgomery County Board of Elections, as well as a representative each of the Pew Trust and FairVote. Following the mock election in April 2009, the SVST proposed a redesigned system taking into considerations feedback

from voters and poll workers (through surveys) and the Board of Elections. In particular, the SVST proposed redesigns of the scanner, the scanner interface and the ballot, and recommended corresponding simpler voting procedures. The Board voted to recommend use of the redesigned system in late July 2009, this was made official in the city election ordinance of late September 2009[5]. Beginning around June 2009, representatives of the Scantegrity Voting System Team (SVST) attended several Board of Election meetings and additionally met many times with the City Clerk and the Chair of the Board of Elections to plan for the election.

The final list of candidates was available approximately a month before the election, on October 2. The Scantegrity *meetings* initializing the data and ballots were held in October (see section 7 for detail), as was a final workshop to test the system. Ballots were delivered in late October. Poll worker training sessions were held by the city on October 28 and 31, and polling on November 3, 2009, from 7 am - 8 pm. The final Scantegrity audits were completed on 17 December 2010; all auditors were of the opinion that the election outcomes were correct (for details see section 7).

3 Scantegrity II

In this section, we given an overview of the Scantegrity II system. For more detailed descriptions, see [9, 10].

Voter Experience. At a high level, the voter experience is as follows. First, a voter checks in at the polling place and receives a Scantegrity II ballot (See Figure 2), along with a privacy sleeve. The privacy sleeve is used to cover the ballot and keep the contents of the voter's ballot private. Inside the voting booth, there is a special "decoder pen" and a stack of blank "voter verification cards". The voter uses the decoder pen to mark the ballot by filling in the bubble next to each of her selections, in the same way as on a conventional optical scan ballot. Marking a bubble with the decoder pen simultaneously leaves a dark mark inside the bubble and reveals a previously hidden confirmation code printed in invisible ink.

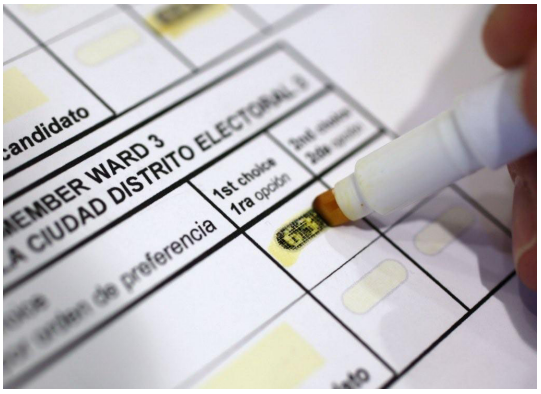
If she wishes to verify her vote later on the election website, the voter can copy her ballot ID and her revealed confirmation codes onto a voter verification card. The voter keeps the verification card for future reference. The voter then takes her ballot to the scanning station and feeds the ballot into an optical scanner, which reads the ballot ID and the marked bubbles.

If a voter makes a mistake, she can ask a poll worker to replace her ballot with a new one. The first ballot is marked "spoiled", and its ballot ID is added to the poll workers' list of spoiled ballot IDs.

The voter can verify her vote on the election website by checking that her revealed confirmation codes and ballot ID have been posted correctly. If she finds any discrepancy, the voter can file a complaint through the website, within the Takoma Park complaint period, which ends at 6 pm on the Friday following the election (a total of approximately seventy hours after the closing of polls). When filing a complaint, the voter must provide the confirmation codes that were revealed on her ballot as evidence of the validity of the complaint. Additionally, any interested party can use software to verify the correctness of the tally on the election website.

Ballots. The Scantegrity II ballot looks similar to a conventional optical scan ballot (see Figure 4 for a sample ballot used in the election). It contains a list of the choices and bubbles besides each one. Inside each bubble is a random 3-digit confirmation code, printed in invisible ink. The confirmation codes are initially hidden. Once a bubble is marked with a decoder pen, the confirmation code is revealed and the bubble is darkened.

[5] See `http://www.takomaparkmd.gov/clerk/agenda/items/2009/090809-3.pdf`, section 2-D, page 2.



INSTRUCTIONS FOR VERIFYING YOUR VOTE ON-LINE AFTER YOU RETURN HOME
PARA LAS INSTRUCCIONES EN ESPAÑOL VEA AL DORSO

You have the **OPTION** of verifying your vote on-line after you return home. **It is not necessary to do so**. You may ignore this step entirely; **your cast ballot will be counted whether or not you do this verification.**

If you wish to verify your vote on-line, perform the following steps:
1. Fill out your ballot according to the instructions provided on the ballot. "Confirmation numbers" will appear inside the ovals you mark.
2. **BEFORE** YOU CAST YOUR BALLOT Record the Online Verification Number and the confirmation numbers below, using the narrow tip of the special pen (note that Wards 1-5 will not have a 3rd choice confirmation number for the city council race).

"On-Line Verification Number" from the bottom right corner of your ballot

Confirmation Numbers	1st Choice	2nd Choice	3rd Choice
Mayor			
City Council Member			

3. **Cast your ballot as usual using the poll-site scanner. DO NOT CAST THIS SHEET, but take it home with you**.
4. After you have returned home, use a computer with an Internet connection to access the City Clerk's web page: **www.takomaparkmd.gov/clerk**. Here you will see instructions for verifying that the confirmation numbers you wrote down are correctly recorded. Note that the confirmation numbers are randomly generated and cannot be used to determine your vote.

Thank you for verifying your vote!
The Takoma Park Board of Elections

Figure 2: Left: a portion of a marked ballot for Ward 3, showing exposed digits of the confirmation number when the decoding ink reacts with the reactive ink in the oval. Notice the chisel tip of the pen. Picture by A. Rivest. Right: The verification card for writing down confirmation numbers. True size is 8.5" x 11"; Spanish instructions were on the back. Because the marking areas are printed on with reactive ink, the same pen can be used to mark the ballot and to note confirmation numbers. A two-sided pen with chisel and regular tips was used for the election.

Confirmation Codes The confirmation codes have the following properties. The codes are unique within each contest on each ballot, and are generated independently and uniformly pseudorandomly. The confirmation code corresponding to any given choice on any given ballot is hidden and unknown to any voter until the voter marks the bubble for that choice.

Backend Prior to the election, a group of election trustees secret-share a seed to a pseudorandom number generator (PRNG). The trustees then input their shares to a trusted workstation to generate the pseudorandom confirmation codes for all ballots, as well as a set of tables of cryptographic commitments used in the backend of the system. These tables allow individual voters to verify that their votes have been included in the tally, and allow any interested party to verify that the tally has been computed correctly, without revealing how any individual voter voted.

Auditing After the election, any interested party can audit the election by using software to check the correctness of the data and final tally on the election website. Additionally, at the polling place on the day of the election, any interested party can choose to audit the printing of the ballots. A print audit consists of marking all of the bubbles on a ballot, and then either making a photocopy of the fully marked ballot or copying down all of the revealed confirmation codes. The ballot ID is recorded by poll workers as audited. After the election, one can check that all of the confirmation codes on the audited ballot, and how the codes correspond to the choices on the ballot are posted correctly on the election website. In order to protect against efforts to cheat by changing the data on the election website, multiple copies of the published data can be maintained by multiple independent entities (such as auditors; this was done by the independent auditors auditing the election, see sections 6 and 7.3 for details).

Elections In addition to the Takoma Park Arbor Day mock election, Scantegrity has been tested in several mock elections, including a survey for Fair Vote's Claim Democracy conference (2007), the Information

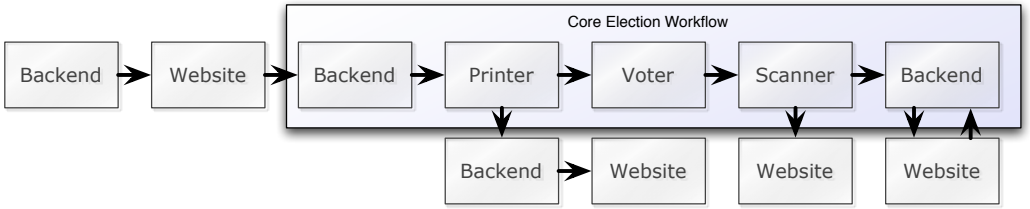


Figure 3: **Election Workflow**. The core election work flow in Scantegrity is similar to an optical scan election: a software backend creates ballot images which are printed, used by voters, and scanned. The results are fed to the backend which creates the tally. The audit capacity is provided by 3 extra steps: (1) create the initial digital audit trail and audit a portion of it, (2) audit the ballots to ensure correctness when printing, and (3) audit the final tally.

Technology and Innovation Foundation's Future of Voting forum (2008), the Ottawa Linux Users Group (2008), and the University of Maryland - College Park (2009).

Note: in the rest of the paper, "Scantegrity" refers to the voting team or to the Scantegrity II voting system; which one is typically easily determined from context.

4 Implementation

The election required a cryptographic *backend*, a *scanner*, and a *website*. These 3 components form the basic election system and their interaction is described in Figure 3. In addition, Takoma Park required software to resolve write-in candidate selections and produce a formatted tally on election night. Each component was written in Java, and we describe the implementation of each one in the following sections.

Backend The cryptographic backend which provides the digital audit trail is a modified version of the Punchscan backend [23]. This backend is written in Java 1.5 using the BouncyCastle cryptography library[6]. We chose the Punchscan backend over newer proposals [9] because it had already been implemented and tested for previous elections [15, 30]. In order to work for Scantegrity, this backend needed modifications that address the linking of confirmation numbers to the input of the backend. For details on how a Punchscan back-end may interface with a Scantegrity front end, see [25].

The Punchscan backend uses a two-stage mix process based on cryptographic commitments published before the election. Each, the *left mix* and the *right mix*, takes coded ballots, shuffles the order, and changes each code according to a prescribed (pre-committed to) permutation to obtain the cleartext votes. Key management in the Punchscan backend is handled by a simple threshold [27] cryptosystem that asks for a username and password from the election officials.

A set of *meetings* was held by election officials using Scantegrity-written software to set up the election, generate ballots and respond to audit challenges. Before the election, during *Meeting 1*, the backend software creates a digital audit trail by committing to a Punchscan representation of candidate choices and to the *mixset*: the left and right mix operations for each ballot. Later, during *Meeting 2*, the backend software responds to an audit of the trail demonstrating that the mixset decrypts ballots correctly. At this time, the backend also commits to the Scantegrity front-end, consisting of electronic ballots (correspondences between candidates and confirmation numbers) and to the linkage between the Scantegrity front-end and its PunchScan backend used for decryption.

[6] `http://www.bouncycastle.org`

Meeting 3, after the election, publishes the election results and the voted confirmation numbers. For the purposes of the tally audit, it also publishes the outputs of the left and right mixes; the latter is simply a shuffled instance of the votes. In *Meeting 4*, the backend software responds to the challenges of the tally computation audit. Either the entire *left mix* or the entire *right mix* operations are revealed, and the auditor checks them against data published in *Meeting 3*. This audit catches, with probability one half, a voting system that cheats in the tally computation. To provide higher confidence in the results, the backend creates multiple sets of left and right mixes; the SVST created 40 for this election, 20 of which were audited.

The Punchscan backend partitions [24] each contest, which means that each contest is treated as an independent election with a separate set of commitments. Therefore, given 2 contests per ballot and 40 sets of left and right mixes, there are a total of 160 commitments per ballot in the audit trail, in addition to a commitment per contestant per ballot for each confirmation number.

The implementation uses two classes of "random" number sources. We describe each.

Audit Trail. The backend requires random numbers to generate the audit trail, which consists of the confirmation numbers, mixes, and commitments. These numbers must be unpredictable to an adversary.

The Punchscan backend generates the mixes and commitments using entropy provided by each election official during initialization of the threshhold encryption. This provided a "seed" for a pseudorandom number generator (based on the SHA-256 hash function

We also used this random source to generate the confirmation numbers when changing the Punchscan backend to support Scantegrity. Unfortunately, we introduced an error in the generation when switching from alphanumeric to numeric codes as a result of the Mock election (5). This resulted in approximately 8.5 bits of entropy as opposed to the expected 10 bits. We discovered this error after we started printing and it was too late to regenerate the audit trail.

Auditing. Random numbers are needed to generate challenges for the various auditing steps (print audit, randomized partial checking). These numbers should be unpredictable in advance to an adversary. They should also be "verifiable" after the fact as having come from a "truly random" source that is not manipulable by an adversary.

We chose to use the closing prices of the stocks in the Dow Jones Industrial Average as our verifiable but unpredictable source to seed the pseudorandom number generator. (the use of stock prices for this purpose was first described in [13]). These prices are sufficiently unpredictable for our purposes, yet verifiable after the fact. However, it turns out that post-closing "adjustments" can sometimes be made to the closing prices, which can make these prices less than ideal for our purposes, in terms of verifiability.

Scanner Software As there was no pre-existing optical scan system to build on top of, we implemented an optical scanning system using netbooks and Fujitsu 6140 scanners. The netbooks ran Ubuntu Linux and automatically started the scanning software.

The scanning software is written in Java 1.6. It uses a bash shell script to call the SANE scanimage program [7] and polls a directory on the filesystem to acquire ballot images. Once an image is acquired it uses circular alignment marks to adjust the image, reads the barcode using the ZXing QRCode Library [8], and uses a simple threshold algorithm to determine if a mark is made on the ballot.

Individual races on each ballot are identified by ward information in the barcode. Write-in candidate areas, if that candidate is selected by the voter, are stored as clipped raw images with the ballot scan results. The results are tagged with a scanner id number and stored in a random location in a memory mapped file on a flash drive. The flash drive is used by the write-in resolution software to acquire and tabulate results from each scanner.

[7] `http://www.sane-project.org/`

[8] `http://code.google.com/p/zxing/`

Tabulator/Write-In Software At the request of Takoma Park, we created an additional piece of software, the Election Resolution Manager, that allows election judges to manually determine for each write-in vote, for which candidate that vote should be counted. An image of the write-in is shown, and the election judge can either type in the name of the intended candidate, or select it from a list of candidates or previous identified write-ins. We call this process *resolving* a vote because the original vote is changed from the generic "Write-In" candidate to the candidate that was intended by the voter.

The ERM acts as part of the backend. After loading each scanner flash drive, the ERM user resolves each write-in candidate. At the end, the results, backend input files, and a PDF file containing all the image clips that were used for resolving as well as the actual candidate names they were resolved to are created.

Website The website has two main purposes: (1) providing voters a mechanism to verify the codes they copied from their ballot against the codes generated by the system during the tally and (2) showing the tallied election results. The website is written in Java 1.6. It uses the Stripes Framework [9] and an apache derby database backend [10].

When officials upload election data the results are available, and a voter can verify her confirmation codes by typing in her ballot serial number— the website then shows the confirmation codes that should be identical to what the voter recorded on her verification card. (If not, the voter can dispute the entries shown, using another portion of the website, or directly to the election auditors.) Ben Adida also provided his own list of verification codes for voters to use [2].

5 Mock Election

A "mock election" was held on Arbor Day to test out the Scantegrity II system. Volunteer voters voted for their favorite tree. Lack of space precludes a full discussion of the mock election here.

A number of revisions and tweaks to the Scantegrity system were made as a result of the mock election, including: ballot revisions (no detachable chit, but instead a separate voter verification card), pen revisions (two-ended, with different sized tips), scanner station revisions (better voter flow, no monitor, two scanners), privacy sleeve (no lock, no clipboard, folding design, feeds directly into scanner), confirmation codes (three decimal digits). The most important changes resulted in a decrease in average voting time from 8 minutes for the mock election down to 2.5 minutes for the real election. For more details on the survey results of the mock election, see [16].

6 Preparing for the Election

Ballots The ballot used for the 2009 election was based on ballots used in past elections, in particular, on a ballot used for the 2007 election. We made the conscious choice to modify (as little as possible) a design already used successfully in a past election, and not to use the special Scantegrity ballot we had designed for the mock election. The main reason for reusing the ballot design was that it would be familiar to voters. The ballot was required to contain instructions in both English and Spanish: marking instructions, instructions for write-ins, instructions for IRV and any Scantegrity-related instructions (see Figure 4).

Early in-person voters used Scantegrity ballots with all Scantegrity functionality, except that the early votes were scanned in after the polls closed on Election Day, and not by voters themselves. Voters were, however, provided verification cards and could check confirmation codes for these ballots online.

[9] `http://www.stripesframework.org/`

[10] `http://db.apache.org/derby/`

Absentee ballots were identical to in-person voting ballots except they did not contain online verification numbers and voters were not given any instructions on checking confirmation numbers online. This was to prevent the possibility of false charges of election fraud by adversaries who might expose confirmation codes and reprint ballots, or use expensive equipment to attempt to determine the invisible codes. (Confirmation numbers for these ballots were, however, made available online after the ballots were scanned, so that there was no distinction in published data between absentee and in-person voted ballots, except that absentee confirmation numbers were not verifiable by voters).

Ballot Printing with Invisible Ink SVST manufactured invisible ink using simple processes available over the internet [11]. SVST created a large batch of ink using yellow dye and added a colorless active ingredient that turns black when exposed to chemicals in the marker used for voting.

We used refillable inkjet cartridges to add the invisible ink to the printer. Yellow and Magenta were replaced with the reactive half of the ink and the unaltered "dummy" ink. We wrote a tool in Java 1.6 called the Inkerator that allowed us to calibrate the two yellow colors in the printer such that they printed indistinguishably. Using these settings we generated ballot PDFs with confirmation numbers as described in [12].

The software we used for printing, PowerRIP [13] allowed us to manipulate the exact intensity of each color printed by each Epson R280 color inkjet printer. We initially began printing with 6 printers, but they proved unreliable. It was our expectation that using a large amounts of commodity hardware would scale, but it did not. We did not anticipate the number of failure modes we experienced and our printing process was delayed by approximately 1 and a half days.

Scanner The scanner was a turn key system. Users only needed to plug in the flash drives and power on the netbooks. The scanner was attached to a scanning apparatus, and cables were run into a lockbox that contained the netbook. When ready, the scanner would beep 3 times. After reading a ballot, the scanner would beep 1 time. During shutdown, the scanner would be another 3 times, and if there were any failure modes the scanner would beep continuously, or not beep at all.

Poll Worker Training Training was held prior to the mock election. Manuals from the previous election were updated and a companion guide was created with Scantegrity-specific instructions. Poll workers were given these two manuals, and the SVST demonstrated the entire voting process. After the mock election, manuals were updated for the final election. Eight poll workers and three members of the Takoma Park Board of Elections received this training.

Voter Education Voter education for this election focused on online verification. Articles in the City newspaper both before the mock election and before the real election indicated that voters could check confirmation numbers online; this was also announced in the city's election ordinance and on the city's election website [29]. Additionally, the mock election also allowed voters to learn about out the system.

Independent Auditors The Board of Elections requested cryptographers Dr. Ben Adida (Center for Research on Computation and Society, Harvard University) and Dr. Filip Zagórski (Institute of Mathematics and Computer Science, Wroclaw University of Technology, Poland) to perform independent audits of the digital data published by Scantegrity in general, and of the tally computation in particular. Dr. Adida [2] and Dr. Zagórski [31] maintained websites describing the audits and the results of the audits, and Dr. Adida

[11] http://www.ehow.com/about_4707862_formula-making-inkjet-ink.html

[12] http://scantegrity.org/~carback1/ink/

[13] http://www.birmy.com/powerrip_x.htm

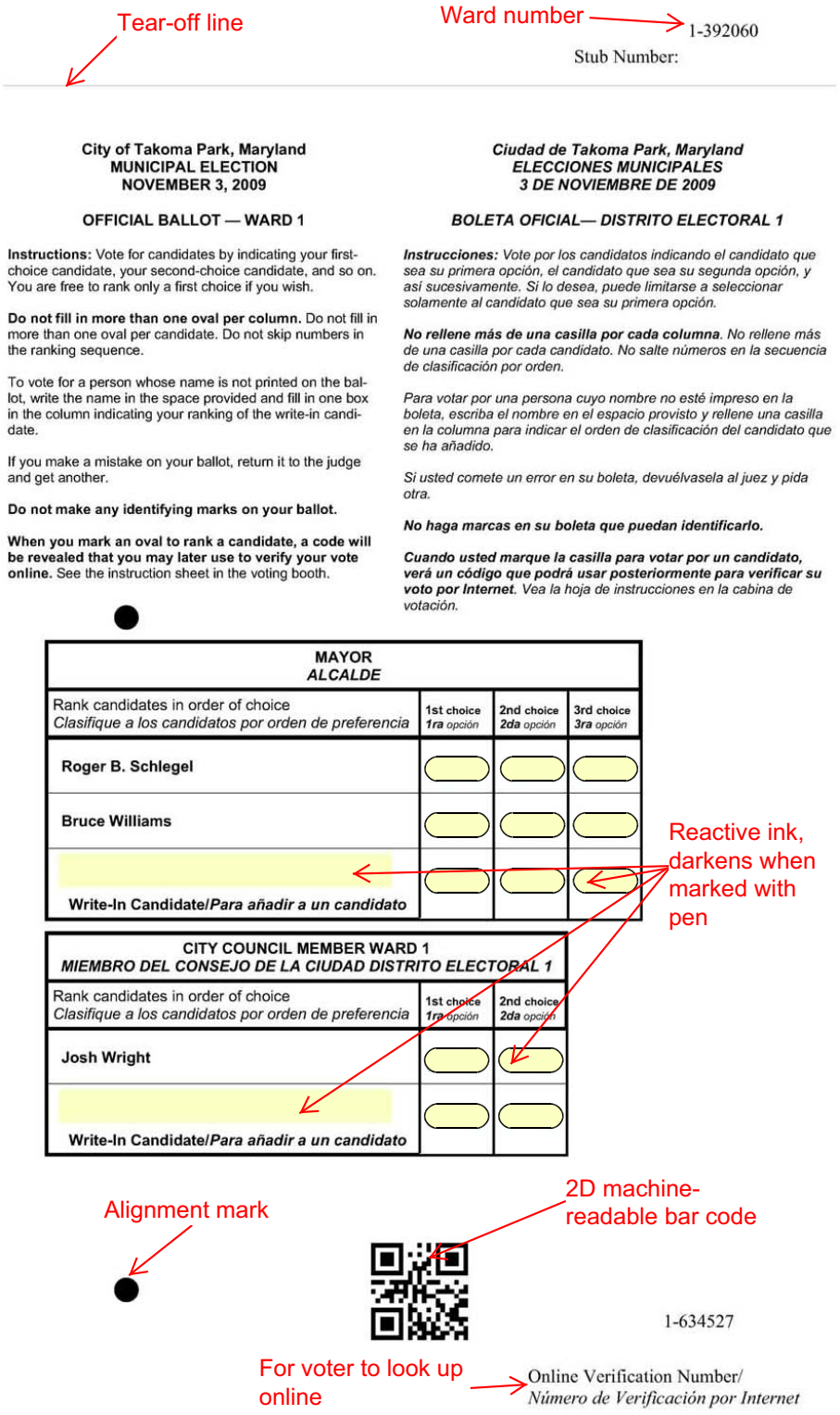


Figure 4: An unmarked Takoma Park 2009 ballot for Ward 1 showing instructions in Spanish and English, the options, the circular alignment marks, the 2D barcode, the ballot serial number (on the stub, meant for poll workers to keep track of the number of ballot used) and the online verification number (for voters to check their codes). The true ballot was printed on legal size paper and was hence larger than shown.

also blogged the audit [1]. Before the election, Dr. Adida pointed out several instances when the Scantegrity information was insufficient; Scantegrity documentation was updated as a result.

The Board of Elections also requested Ms. Lillie Coney (Associate Director, Electronic Privacy Information Center and Public Policy Coordinator for the National Committee for Voting Integrity (NCVI)) to perform print audits on Election Day. Ms. Coney would choose ballots at random through the day, expose the confirmation codes for all options on the ballot, and kept these with her till after the end of the complaint period, when Scantegrity would open commitments to all unvoted and unspoiled ballots (and hence to all ballots she had audited). Ms. Coney would then check that the correspondence between codes and confirmation numbers on her ballots matched those on the website.

Both tasks, of print audits and digital data audits, can be performed by voters. Digital data audits can also be performed by any observers. In future elections, when the general population and Takoma Park voters are more familiar with the power of end-to-end elections, it is anticipated that voters (and, in particular, candidate representatives) will perform such audits.

7 Conducting the Election

In this section, we describe the activities around the election itself. In particular, we describe the use of the Scantegrity software to generate the digital audit trail and the ballots, the election itself, and activities after the election to corroborate the Scantegrity count.

7.1 Election Set-Up

The main activities for setting up the election included formal *meetings* 1 and 2, which established the election trustees and the digital audit trail for the ballots, as well as the printing of the ballots.

Four election officials (the City Clerk, the Chair, Vice Chair and a member of the Board of Elections: Jessie Carpenter, Anne Sergeant, Barrie Hofmann and Jane Johnson, respectively) were established as election trustees in *Meeting 1*, held on October 12 2009 (see Figure 1). It was explained to the trustees that, through their passwords, they would generate the confirmation codes and share the secret used to tally election results. Further, it was explained that, without fewer than a threshold of passwords the election could not be tallied by Scantegrity, and that if a threshold number of passwords was not accessible (if they were forgotten, for example, or trustees were unavailable due to sickness) the only available counts would be manual counts. A threshold of two trustees was determined based on anticipated availability of the officials, and it was explained that two trustees could collude to determine the correspondence between confirmation numbers and codes, and hence that each trustee should keep her password secret. During Meeting 1, using code written by Scantegrity, the trustees generated commitments to the decryption paths for each of 5000 ballots per ward (for six wards). Scantegrity published the commitments.

In *Meeting 2*, held on October 14, 2009, trustees used Scantegrity-written code to respond to challenges generated using stock market data at closing on October 14. Half of the ballot decryption paths committed to in Meeting 1 were opened. Additionally, trustees constructed ballots (associations between candidates and confirmation codes) at this meeting, and generated commitments to them. Scantegrity published the stock market data, the challenges, and the responses.

Mail-in (absentee) ballots were delivered to the City Clerk on 16 October; early, in-person voting ballots on October 27 for early voting on October 28, and all ballots a couple of days later.

7.2 The Election and Certification

Election Day On Election Day, November 3, 2009, polls were open from 7 am to 8 pm at a single polling location, the Takoma Park Community Center. Several members of the SVST were present through most of

the day in the building in case of technical difficulty, one SVST member was present in the polling room at most times as an observer, and a couple of SVST members were present in the vestibule giving out and collecting survey forms through most of the day. Lillie Coney of the Electronic Privacy Information Center, who performed a printed ballot audit on request by the Board of Elections, was present in the polling room through a large part of the day. Ms. Coney chose about fifty ballots at random, uniformly distributed across wards, and exposed the confirmation codes for all options for the ballots. A copy of each ballot was made for her to take with her; the copies wee signed by the Chair of the BoE. Neither Ms. Coney nor SVST members had any interaction with voters.

The election proceeded quite smoothly, with very few, small glitches. An SVST member was able to assist polling officials in fixing a problem with their poll books (not provided by Scantegrity). Voters had some initial problems with the use of the scanner and the privacy sleeve, some seeking assistance from poll workers. After an explanation to the poll workers by the Chair of the Board of Elections, the use of the scanner was considerably smoother. With a few ballots, the privacy sleeve was not letting go of the ballots; one ballot was mangled considerably but scanned fine. About fifteen scanned ballots, scanned in a time period of about seventy-five minutes by the same scanner, had lines on them that caused the scanner to be unable to read votes. Images of all scanned ballots were saved, and those not readable by the scanner were marked, so we were able to manually enter in these votes. We believe this combination of problems is consistent with there being something sticky on a ballot, left on from a voter's hands. These problems did not affect our ability count the votes.

Towards the end of the day, after the local NPR station carried clips from an interview with the Chair of the Board of Elections and a voter, the polling station saw a large increase in the number of voters, with the line taking up much of the lower floor of the polling location. Some voters were curious about the verifiability properties of the system. The SVST prepared to print more ballots, but this was not required. The number of printed ballots ended up being almost twice the number of voted ballots.

Absentee and early voted ballots were scanned in after the closing of polls, and, in *Meeting 3a*, trustees used Scantegrity code to generate results without provisional ballots at about 10 pm. The Chair of the Board of Election announced the results to those present at the polling place at the time (including candidates, their representatives, voters, etc.); this was also televised live by the local TV station. Confirmation codes and the election day tally were posted on the Scantegrity website. At a later date, Dr. Adida [2] and Dr. Zagórski [31] also made the confirmation codes available on their websites.

Final Electronic Count On the next day, around 2 pm, results including verified provisional ballots were determined by trustees using Scantegrity code. (These results were published by Scantegrity.) Takoma Park representatives announced a tally without provisional ballots first, followed by the tally that included verified provisionals, in accordance with standard Takoma Park procedures.

Hand Count and Certification Following a hand count performed by representatives from both the SVST and Takoma Park, the Chair of the Board of Elections certified the results of the hand count to the City Council at 7 pm. on November 5. The hand count and the Scantegrity count differed very slightly because we were able to better determine voter intent during the hand count. For example, voters would occasionally write-in a vote without filling in a write-in oval; this was considered a write-in vote during the hand count, but not by Scantegrity software.

The hand count was very important as it was the only audit of Scantegrity's electronic count that preceded certification. Scantegrity audits could not be held till all voters had been given a chance to complain about missing or manipulated confirmation codes, and the election is typically certified the day after it is held. For a system and a paradigm (end-to-end voting) that had not been tested before in a governmental election, and that enforced greater accountability, it was particularly important to allow election officials to

perform an audit prior to certification. The hand count was also an opportunity for the SVST to experience an important aspect of a regular election, and to observe the types of differences between hand count and machine count results, such as those from the interpretation of voter intent.

7.3 After the Election

The period for complaints regarding the election (including complaints about missing confirmation codes) expired at 6 pm on November 6. The Scantegrity website has recorded 81 unique ballot ID verifications, of which about 66 (almost 4%, see section 8) were performed before the deadline. The SVST was also told by a BoE member that at least a few voters checked codes on auditor websites. Scantegrity received a single complaint by a voter who had trouble deciphering a digit in the code, noted it as "0", while the Scantegrity website presented it as '8". The voter requested that codes be printed more clearly in the future. He also stated that if he were not a trusting individual, he would believe that he had proof that his vote was altered. All codes for all voted ballots were revealed after the dispute resolution period (see next paragraph), and all commitments verified by two independent auditors, Dr. Adida and Dr. Zagórski. Hence, the probability that the code was in error is very small, albeit non-zero. Scantegrity does not believe the code was in error, and there were no other complaints.

During *Meeting 4*, held on November 6 at 6 pm., trustees used Scantegrity-written code to reveal all codes on voted ballots, and to reveal everything for all the ballots that were not spoiled or voted upon. Trustees also used Scantegrity-written code to respond to pseudo-random challenges generated by Scantegrity code using stock market results at closing on November 6. Scantegrity published all generated data. While the SVST could have chosen to use closing data on an earlier date, such as November 4 or November 5, which could have been more stable, the team chose to stick to its earlier-announced plan (of using the freshest stock market data) for the sake of consistency.

On November 9, 2009, Dr. Adida and Dr. Zagórski independently confirmed that Scantegrity correctly responded to all digital challenges. In particular, that the tally computation audit data was correct. Both made available independently-written code on their websites that voters and others could use to check the tally computation commitments. The Chair of the BoE mentions that several voters have shown an interest in running the code made available by Drs. Adida and Zagórski, and that she expects that Takoma Park voters will use the code to perform some audits themselves in the next few months.

Dr. Zagórski provided an interface allowing Ms. Coney to check the commitments opened by Scantegrity in Meeting 4 against the candidate/confirmation-code correspondence on the ballots she audited. In her report [14], she confirmed that the correspondence between confirmation numbers and candidates on all the printed ballots audited by her was correctly provided by the interface.

The Board of Elections and an SVST representative met to discuss the election and opportunities for improvement. Both sides were largely satisfied with the election. Conversations have begun regarding the use of Scantegrity in the next municipal election at Takoma Park, to be held in November 2011. No decisions have been taken.

8 Election Outcome

The number of registered voters were 10,934 and 1728 votes were cast (15.8%). The city-certified final tally for each contest is provided below. In each race, a majority was won after tallying after the voter's first choice.

Mayor	Votes	Ward	Councilor	Votes	Ward	Councilor	Votes
Roger B. Schlegel	664	Ward 1	Josh Wright	434	Ward 4	Terry Seamens	196
Bruce Williams	1000		Write-ins	13		Eric Mendoza	12
Write-ins	17	Ward 2	Colleen Clay	236		Write-ins	2
			Write-ins	15	Ward 5	Reuben Snipper	71
		Ward 3	Dan Robinson	397		Write-ins	10
			Write-ins	34	Ward 6	Navid Nasr	61
						Fred Schultz	138
						Write-ins	0

The number of voters who checked their ballots on-line (66), while not large, was sufficient to have detected (with high probability) any errors or fraud large enough to have changed the election outcome. (Detailed calculations omitted here; these calculations are not so simple, due to the use of IRV.)

9 Surveys and Observations of Voter Experiences

To understand the experiences of voters and poll workers, we timed some of the voters as they voted, asked voters and poll workers to fill out two questionnaires, and informally solicited comments from voters as they left the precinct building. Approved by the Board of Elections and UMBC's Institutional Review Board, our procedures respected the constraint of not interfering with the election process. This section summarizes the results of our observations and surveys.

Timing Data Sitting unobtrusively as official observers in a designated area of the polling room for part of the day, two helpers (not members of the Scantegrity team) timed 93 voters as they carried out the voting process. Using stopwatches, they measured the number of seconds that transpired from the time the voter received a ballot to the time the voter began walking away from the scanner.

Voting times ranged from 55 secs. to 10mins. (the second longest time was 385 secs.), with a mean of 167 secs. and a median of 150 secs. On average, voters who appeared older took longer than voters who appeared younger. Most of the time was spent marking the ballot. The average time to vote was significantly faster than during the April 2009 mock election, when voters took approximately 8 mins. on average due primarily to scanning delays [16].

The observers noted that many voters did not fully use the privacy sleeve as intended, removing the ballot before scanning rather than inserting the privacy sleeve with ballot into the scanning slot. Two of the 93 observed voters initially inserted the privacy sleeve upside-down, causing the ballot not to be fed into the scanner (even though the scanner could read the ballot in any orientation). A few ran into difficulties trying to insert the sleeve with one hand while holding something else in the other hand.

Election Day Comments From Voters As voters left the precinct building, members of the Scantegrity team conducting the written surveys, and a helper (a usability expert who is not a member of the Scantegrity team) solicited comments from voters with questions like, "What did you think of the new voting system?" The helper solicited comments 1:30-3:00pm and 7-8pm. A common response was, "It was easy."

Quite a few voters did not understand that they could verify their votes on-line and that, to do so, they had to write down the codenumbers revealed by their ballot choices. Some explained that they intentionally did not read any instructions because they "knew how to vote." Others failed to notice or understand instructions on posters along the waiting line, in the voting booth, on the ballot, and in the Takoma Park Newsletter.

In response, later in the day, we announced to voters as they entered the building that there is a new system; to verify your vote, write down the codenumbers. These verbal announcements seemed to have some positive effect, and there were fewer voter comments expressing lack of awareness of the verification

option after we began the announcements. Nevertheless, some voters still were unaware of the verification option. It was a humbling experience to see first-hand how difficult it can be to get across the most basic points effectively, especially the first time a new system is used.

Some of the voters complained about the double-ended pen, not knowing which end to use, or having trouble writing in candidates with the chisel-point (the narrow point was intended for write-ins). A small number of voters had difficulty seeing the codenumbers, perhaps largely because repeatedly pressing too hard could erode the paper. A few voters expressed concern about the difficulty of writing down the codenumbers, had the ballot been much longer or had there been a large number of competing candidates.

Many voters expressed a strong confidence in the integrity of elections, while a small minority expressed sharp distrust in previous electronic election technology. These feelings seemed to be based more on a general subjective belief rather than on detailed knowledge of election procedures and technology. Similarly, those expressing strong confidence in Scantegrity seemed to like the concept verification but did not understand in detail why Scantegrity provides high outcome assurance.

Survey of Voter Experiences As voters were leaving the precinct, we invited them to fill out two one-sided survey forms: a field-study questionnaire, and a demographics questionnaire. The field study asked voters about the voting system they just used, with most answers expressed on a seven-point Likert scale. The last question invited voters to make any additional suggestions or comments. Each pair of forms had matching serial numbers to permit correlation of the field study responses with demographics. 271 voters filled out the forms.

Twenty-nine voters wrote comments on the questionnaires, often pointing out confusion about various aspects of the process. (1) Some were unaware of verification option. (2) Some did not realize they were supposed to write down codenumbers. (3) Some found the pens confusing to use: they did not realize that the pens would expose codenumbers, and they did not know which end to use. (4) Some found codenumbers were hard to read. (5) Some did not understand how to mark an IRV ballot. (6) Some did not know how to place the ballot into the scanner. (7) One had no difficulty but wondered if seniors or people who speak neither English nor Spanish might have difficulties. (8) One wondered if the government might be able to discern his vote by linking his IP address used during verification with his ballot serial number and noting the time that he was issued a ballot. (9) Many suggested that it would have been helpful to have better instructions, including instruction while they wait in line.

Figure 5 shows how voters responded to four questions from the field study questionnaire. These results strongly show that voters found the voting system easy to use (Question 5), and that they had confidence in the system (Question 13). Question 10 showed that the option to check votes on line increased voter confidence in the election results. Question 9 showed that voters had confidence that the receipt alone did not reveal how they voted; this finding is notable given that it is widely suspected that many people erroneously believe that all e2e receipts reveal ballot choices. We plan to present detailed analysis of our complete survey data in a separate companion paper.

Survey of Poll Worker Experiences Each of the twelve poll workers was given an addressed and stamped envelope with two questionnaires (field study and demographics) to fill out and mail to the researchers after the election. The field study focused on their experiences administering Scantegrity, with most answer expressed on a seven-point Likert scale. This questionnaire also included four open-ended questions. Each pair of forms had matching serial numbers. Five forms were returned.

Poll workers noted the following difficulties. (1) There was too much information. (2) Some voters did not understand what to do, including how to create a receipt. (3) Some voters did not understand how to mark an IRV ballot. (4) The privacy sleeve was hard to use with one hand. (5) The double-ended pens created confusion. (6) Voters, poll workers, and the Scantegrity team have different needs. One wondered if

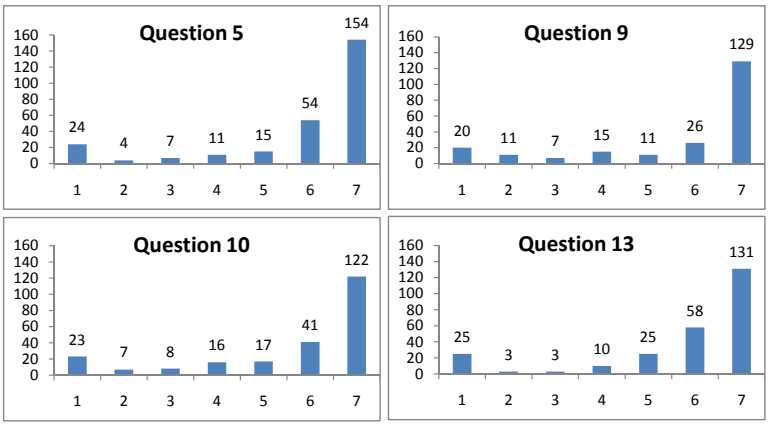


Figure 5: Voter responses to Survey Questions 5, 9, 10, 13 from all 271 voters completing the survey. Using a seven-point Likert scale, voters indicated how strongly they agreed or disagreed with each statement about the voting system they had just used (1 = strongly disagree, 7 = strongly agree). Each histogram shows the number of voters responding for each of the seven agreement levels. The four questions shown are the following: (5) Overall, the voting system was easy to use. (9) I have confidence that my receipt by itself does not reveal how I voted. (10) The option to verify my vote online afterwards increases my confidence in the election results. (13) I have confidence in this voting system.

Scantegrity was worth the extra trouble.

They offered the following suggestions: (1) Simplify the ballot. (2) Provide receipts so that voters do not have to copy codenumbers. (3) Develop better pre-election voter education.

10 Discussion and Lessons Learned

Overall, this project should be deemed a success: the goals of the election were met, and there were no major snafus. Many aspects of the Scantegrity design and implementation worked well, while some could be improved in future elections.

Perhaps the most challenging aspect for future elections is scaling up ballot printing. The printers we used were not very reliable.

As is common with many projects, too much was left until the last minute. Better project management would have been helpful, and key aspects should have been finalized earlier. Materials and procedures should be more extensively tested beforehand.

Variations on the Scantegrity design worth exploring include the printing of voter receipts (rather than having voters copy confirmation codes by hand)—there are clearly security aspects to handle if one does this. The design should also be extended for better accessibility. It might also be worthwhile to have an instructional video explaining the Scantegrity system that voters could watch as they come in. The special pen might be improved by having only a single medium-tip point, rather than two tips of different sizes. The scanning operation and its interaction with the privacy sleeve should be studied and improved.

Perhaps one of the most important lessons is the value of close collaboration and teamwork between election officials and the election system providers (whether they be researchers or vendors).

11 Related Work

Chaum was the first to propose the use of cryptography for the purpose of secure elections [7]. This was followed by almost two decades of work in improving security and privacy guarantees (see for example, the overview in [3]), most recently under the rubric of *end-to-end* voting systems. These voting system proposals provide integrity (any attempt to change the tally can be caught with very high probability by audits which are not restricted to privileged individuals) and ballot secrecy which holds even if the voter chooses to collude with the adversary (such as due to a threat or a bribe). While such systems are quite varied, they often include the notion of an electronic "bulletin board" where data is made public in an irrefutable and unalterable manner.

The first of these proposals include *Votegrity* [8] and the protocol of Neff [21], which were implemented soon after (*Votegrity* as *Citizen-Verified Voting* [18] and Neff's protocol by VoteHere). Several more proposals with prototypes followed: *Prêt à Voter* [12], *Punchscan* [23, 17], the proposal of Kutylowski and Zagórski [20] as *Voting Ducks*, and Simple Verifiable Voting [6] as *Helios* [4] and *VoteBox* [26].

The case study reported here is based on a series of systems successively developed, tested and deployed by a team of researchers included among the present authors. The *Punchscan* system was deployed for the annual general election of the graduate students' union of the University of Ottawa in 2007 [15]. (For this, the team won first prize at the *VoComp*, Voting System Competition in 2007 [30]). However, the *Punchscan* system did not allow hand count, a feature that the team recognized as needing to be designed into the next generation of systems. The result was *Scantegrity* [11], which retained physical ballots, and was tested in a number of small elections. With *Scantegrity*, however, it was too easy to trigger an audit that would require scrutiny of the physical ballots. The *Scantegrity II* system [9, 10], deployed in Takoma Park, was a further refinement to address this problem by allowing a public statistical test of whether voter complaints actually reflect a discrepancy or whether they are without basis.

Actually making end-to-end systems so they may be used in real elections has proven to be challenging. The only previous binding elections that we are aware of held using E2E systems with freely-available code are: the *Punchscan* elections for the graduate students' union of the University of Ottawa (2007) and the Computer Professionals for Social Responsibility[14] (2007); the Rijnland Internet Election System (RIES) public elections in the Netherlands in 2004 and 2006; the *Helios* election of the Recteur of Université Catholique de Louvain [5] (2009) and the Princeton undergraduate student government election (2009), as well as a student election using *Prêt à Voter*. Of these, only the RIES system has been used in a governmental election; however, it is meant for remote (absentee) voting and, consequently, does not offer strong ballot secrecy guarantees. For this reason, it has been recommended that the RIES system not be used for regular public elections [19, 22].

12 Conclusions

Traditional opscan voting systems have the clear benefit that "votes are verifiably cast as intended"—the voter can see for herself that the ballot is correctly filled out. Yet once her ballot is cast, the voter must place her trust in others that ballots are safely collected and correctly counted. With end-to-end voting systems these last two operations (collecting ballots and counting them) are verifiable as well: voters can verify—using their receipt and a website—that their ballot is safely collected with the others, and anyone can use the website data to verify that the ballots have been correctly counted. The Scantegrity II voting system provides such end-to-end verification capability as an overlay on top of traditional opscan technology, obtaining both the familiarity and security benefits of opscan with the augmented integrity guarantees of end-to-end voting.

[14] See `http://punchscan.org/cpsr2007/index.php.html`.

Further development should improve scalability (esp. printing), usability (e.g. with printed receipts) and accessibility of the Scantegrity II system.

The successful use of the Scantegrity II voting system in the Takoma Park election of November 3, 2009 demonstrates that voters and election officials can take advantage of the most sophisticated cryptographic techniques to organize a secret ballot election with unprecedented transparency, while continuing to enjoy a mostly familiar voting experience. The election results show considerable satisfaction by both voters and pollworkers with this new voting system, and this shows that end-to-end voting technology has matured to the point of being ready and usable for real binding governmental elections. This paper thus documents a significant step forward in the security and integrity of voting systems, as used in practice.

Acknowledgments

The authors would like to acknowledge the contributions of the voters of Takoma Park, the City Clerk, all Board of Elections members since 2008 when this project was first proposed, and the independent auditors—Lillie Coney, Ben Adida and Filip Zagórski—to the success of the election. Additionally, they would like to thank the following. Vivek Relan and Bhushan Sonawane timed voters as they voted and helped assemble the privacy sleeves. Lynn Baumeister interviewed some voters as they left the precinct. Cory Jones provided general assistance and Alex Florescu and Jan Rubio assisted with ink creation.

Alan T. Sherman was supported in part by the Department of Defense under IASP grants H98230-08-1-0334 and H98230-09-1-0404. Poorvi L. Vora was supported in part by The National Science Foundation under grant CNS 0831149.

References

[1] Ben Adida. Benlog: Takoma Park 2009. `http://benlog.com/articles/category/takoma-park-2009/`.

[2] Ben Adida. Takoma Park 2009 Cryptographic Election Audit. `http://sites.google.com/site/takomapark2009audit/`.

[3] Ben Adida. *Advances in Cryptographic Voting Systems*. PhD thesis, MIT EECS Dept., 2006.

[4] Ben Adida. Helios: web-based open-audit voting. In *Proceedings of the 17th USENIX Security Symposium*, pages 335–348, 2008.

[5] Ben Adida, Olivier deMarneffe, Olivier Pereira, and Jean-Jacques Quisquater. Electing a university president using open-audit voting: Analysis of real-world use of Helios. August 2009.

[6] Josh Benaloh. Simple verifiable elections. In *Proceedings of the 2006 USENIX/ACCURATE Electronic Voting Technology Workshop*, Berkeley, CA, USA, 2006. USENIX Association.

[7] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–90, 1981.

[8] David Chaum. Secret-ballot receipts: True voter-verifiable elections. *IEEE Security and Privacy*, 2(1):38–47, 2004.

[9] David Chaum, Richard Carback, Jeremy Clark, Aleksander Essex, Stefan Popoveniuc, Ronald L. Rivest, Peter Y. A. Ryan, Emily Shen, and Alan T. Sherman. Scantegrity II: end-to-end verifiability for optical scan election systems using invisible ink confirmation codes. In *Proceedings of the 2008 USENIX/ACCURATE Electronic Voting Technology Workshop*, pages 1–13, 2008.

[10] David Chaum, Richard T. Carback, Jeremy Clark, Aleksander Essex, Stefan Popoveniuc, Ronald L. Rivest, Peter Y. A. Ryan, Emily Shen, Alan T. Sherman, and Poorvi L. Vora. Scantegrity II: End-to-End Verifiability by Voters of Optical Scan Elections Through Confirmation Codes. *IEEE Trans. on Information Forensics and Security, special issue on electronic voting*, 4(4):611–627, Dec. 2009.

[11] David Chaum, Aleksander Essex, Richard Carback, Jeremy Clark, Stefan Popoveniuc, Alan T. Sherman, and Poorvi Vora. Scantegrity: End-to-end voter verifiable optical-scan voting. *IEEE Security and Privacy Magazine*, 6(3):40–46, May/June 2008.

[12] David Chaum, Peter Y.A. Ryan, and Steve A. Schneider. A practical, voter-verifiable, election scheme. Technical Report Series CS-TR-880, University of Newcastle Upon Tyne, December 2004.

[13] Jeremy Clark, Aleksander Essex, and Carlisle Adams. Secure and observable auditing of electronic voting systems using stock indices. In *Proceedings of the 2007 IEEE Canadian Conference on Electrical and Computer Engineering*, 2007.

[14] Lillie Coney. Report on the Manual Ballot Audit: Takoma Park, Maryland, November 3 2009 Election, 19 November 2009. Electronic Privacy Information Center, `http://epic.org/privacy/voting/takoma_park_audit.pdf`.

[15] Aleks Essex, Jeremy Clark, Richard T. Carback, and Stefan Popoveniuc. Punchscan in practice: an e2e election case study. In *Proceedings of the 2007 IAVoSS Workshop on Trustworthy Elections*, 2007.

[16] Alan T. Sherman et al. Scantegrity mock election at takoma park (summary), October 2009. Presented at End-to-End Voting Systems Workshop Organized by the National Institute of Standards and Technology `http://csrc.nist.gov/groups/ST/e2evoting/documents/papers/SHERMAN_scantegrity%20at%20Takoma-NIST%20revised9-25-09.pdf`.

[17] Kevin Fisher, Richard Carback, and Alan T. Sherman. Punchscan: Introduction and system definition of a high-integrity election system. In *Proceedings of the 2006 IAVoSS Workshop on Trustworthy Elections*, 2006.

[18] Ben Hosp, Nils Janson, Phillipe Moore, John Rowe, Rahul Simha, Jonathan Stanton, and Poorvi Vora. Citizen-verified voting. Presentation at DIMACS Workshop on Electronic Voting – Theory and Practice, May 2004, `http://dimacs.rutgers.edu/Workshops/Voting/slides/vora.ppt`.

[19] Engelbert Hubbers, Bart Jacobs, Berry Schoenmakers, Henk van Tilborg, and Benne de Wege. Description and analysis of RIES, June 2008.

[20] Miroslaw Kutylowski and Filip Zagórski. Verifiable internet voting solving secure platform problem. In *Advances in Information and Computer Security, Lecture Notes in Computer Science*, volume 4752, pages 199–213, 2007.

[21] C. A. Neff. Practical high certainty intent verification for encrypted votes, 2004.

[22] Office for Democratic Institutions and Human Rights. The Netherlands Parliamentary Elections 22 November 2006 OSCE/ODIHR Election Assessment Mission Report, March 12 2007. 28 pages.

[23] Stefan Popoveniuc and Ben Hosp. An introduction to punchscan. In *Proceedings of the 2006 IAVoSS Workshop on Trustworthy Elections*, 2006.

[24] Stefan Popoveniuc and Jonathan Stanton. Undervote and pattern voting: Vulnerability and a mitigation technique. In *IAVoSS Workshop On Trustworthy Elections (WOTE 2007)*, University of Ottawa, Ottawa, Canada, June 2007.

[25] Stefan Popoveniuc and Poorvi L. Vora. A framework for secure electronic voting. In *Proceedings of the 2008 IAVoSS Workshop on Trustworthy Elections*, 2008.

[26] Daniel R. Sandler, Kyle Derr, and Dan S. Wallach. VoteBox: a tamper-evident, verifiable electronic voting system. In *Proceedings of the 17th USENIX Security Symposium*, 2008.

[27] Adi Shamir. How to share a secret. *CACM*, 22(11):612–613, Nov 1979.

[28] City of Takoma Park, Maryland City Election November 3, 2009 Certification of Election Results, November 2009. `http://www.takomaparkmd.gov/clerk/election/2009/results/2009cert.pdf`.

[29] Election 2009, 2009. `http://www.takomaparkmd.gov/clerk/election/2009/`.

[30] VoComp Voting System Competition. July, 2007. Portland, Oregon. `http://www.vocomp.org`.

[31] Filip Zagórski. Scantegrity AUDITOR. `http://zagorski.im.pwr.wroc.pl/scantegrity/`.